Wyoming
Department
of Health

Commit to your health.
visit www.health.wyo.gov

Thomas O. Forslund, Director | **Governor Matthew H. Mead**

Policy Title:	Risk Analysis and Management
Policy Number:	S-001a
Effective Date:	April 1, 2013
Approval:	Thomas O Forslund — 3/14/13 Thomas O. Forslund, Director — Date

Purpose:

This Policy establishes the Wyoming Department of Health's (WDH) responsibility for and approach to analyzing and managing risks and vulnerabilities to electronic protected health information (ePHI) that is housed on WDH systems.

Scope:

Any review processes identified within this Policy, including risk analysis, risk assessments, and risk management may be conducted on any WDH system. WDH's business associates are responsible for appointing their own security officer, implementing their own policies and procedures, and conducting their own risk analysis and management of their systems that house WDH's ePHI.

Policy:

1. **General**
   a. WDH shall conduct periodic risk assessments to identify risks and vulnerabilities to the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits.
   b. Prior to systems placed into production, WDH shall conduct immediate risk assessments for new installations or significant modifications to its systems that maintain ePHI (i.e., software installation, SharePoint pages, newly implemented programs).
      i. For all such proposed new installations or significant modifications, WDH divisions/programs/facilities shall submit a privacy threshold analysis (PTA) and/or a privacy impact assessment (PIA) to the WDH Compliance Office. The WDH Compliance Office must review and approve the PTA and/or PIA before the new installation or significant modification is implemented.
   c. WDH shall reduce identified risks and vulnerabilities to an acceptable level based on a "reasonable and appropriate standard."
2. Risk assessments shall determine, at a minimum, the following information:
   a. The level of risk associated with each identified vulnerability;
   b. Actions necessary to reduce the risk of vulnerability exploitation; and
   c. Actions necessary to achieve and maintain no less than the acceptable level of risk.
3. The WDH Compliance Office shall be responsible for oversight of the risk analysis and management process. The WDH Security Officer shall assume primary responsibility for the process, and the WDH Compliance Officer shall be available to assist with the process.

4. All applicable WDH employees and workforce shall be trained regarding their responsibilities and duties to reduce the risk of security incidents.

Procedures:

1. **Risk Analysis procedures**
    a. Identify WDH's assets (i.e., hardware, software, applications, information/data sets) and perform a criticality analysis; determine the value and relative desired assurance levels. Consider the levels desired for confidentiality, integrity and availability. Ensure ePHI components are identified, and role base classifications are assigned.
    b. Conduct periodic risk assessments of the identified assets by:
        i. Identifying the vulnerabilities to which each of the above assets may be exposed. Consider technical, administrative/process, human and physical vulnerability sources. Include vulnerabilities that could impact the confidentiality, integrity and availability (CIA) of data.
        ii. Identifying the threats that could exploit the vulnerabilities identified. Consider human (intentional and unintentional) and environmental (e.g., weather, air quality) threats. Include threats that could impact the CIA of data.
        iii. Estimating the likelihood that a threat would successfully exploit each of the identified vulnerabilities, given the current countermeasures in place to guard against such exploits.
        iv. Computing the annual loss expectancy for each vulnerability exploitation, equal to the product of the annual probability of loss and the loss expected from a single rate of occurrence.
        v. Surveying the controls and costs of safeguards (physical, technical and administrative). Incorporate safeguards that produce an expected annual cost savings based on the annual loss expectancy, or are otherwise necessary to meet the requirements of security controls selected, considering factors specific to WDH (e.g., size, environment, operating changes and configuration).
2. **Risk Management procedures**
    a. Ensure personnel are adequately trained with respect to information security policies and procedures, including relevant threats, vulnerabilities and countermeasures.
    b. Leverage the results of information system activity reviews and evaluation programs to identify and address areas of deficiency.
    c. Once safeguards have been incorporated based on the outcome of the risk analysis process, identify any residual risk(s). Then, analyze the applicable threats, vulnerabilities and countermeasures for the residual risk.
    d. Based on the probability of occurrence and the value of the applicable asset(s), determine if the residual risk is acceptable. If it is not, continue assessing countermeasure options, including processes, technologies and approaches to reduce the risk to an acceptable level.
    e. Base secure controls and residual risk tolerance on factors specific to WDH (e.g., size, environment, operating changes and configuration). Formulate a scale for determining that which is "reasonable and appropriate." Ensure CIA considerations are made.

Contacts:

De Anna Greene, CIPP/G, CIPP/IT, WDH Privacy/Compliance Officer (307)777-8664
Tate Nuckols, JD, WDH Security Officer (307) 777-2438

Policies:

Security Management Process; S-001
Privacy Threshold Analysis and Privacy Impact Assessment; S-024

References:

45 CFR 164.308(a)(1)(ii)(A)
45 CFR 164.308(a)(1)(ii)(B)

Training: